Brooklyn Law Review

Volume 74
Issue 3
SYMPOSIUM:
The Products Liability Restatement: Was it a Success?

Article 17

2009

Dirty Digits: The Collection of Post-Cut-Through Dialed Digits Under the Pen/Trap Statute

Marcus M. Baldwin

NOTES

Dirty Digits

THE COLLECTION OF POST-CUT-THROUGH DIALED DIGITS UNDER THE PEN/TRAP STATUTE

INTRODUCTION

Telephone users commonly pay outstanding bills or verify bank account balances by navigating an automated system and entering the appropriate digits. In some cases, a caller might dial digits to input personal information, such as a social security number or a pin number to access confidential accounts.[1] Nevertheless, many telephone users would be disturbed to learn that law enforcement agencies may record and store indefinitely all of the digits dialed from a specific telephone without a warrant, without notification to the user, and without a showing of probable cause.[2]

The device that enables law enforcement agencies to collect the outgoing digits a telephone user dials is called a pen register.[3] Though at one time pen registers exclusively monitored telephones, today pen registers monitor communications conducted over a variety of electronic media.[4] In the case of telephones, a pen register can record both the digits dialed to connect a telephone call to its destination and the digits dialed after connection occurs, such as those dialed to navigate automated

---

[1] *In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007). Because the names of the published orders this Note discusses are unwieldy, this Note will refer to the orders by the jurisdiction in which they were decided. Where a district has published more than one order, roman numerals indicate the chronological order in which the orders were issued.

[2] *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 180 (1998).

[3] *Id.* at 117. Pen registers perform the inverse function of trap-and-trace devices, which collect information about all calls received by a particular telephone. *Id.* The Pen/Trap Statute regulates both pen registers and trap-and-trace devices. *See* 18 U.S.C. §§ 3121-3127 (2006) ("Pen/Trap Statute"). The statutory definition of a pen register is located in 18 U.S.C. § 3127(3) ("Definition") and discussed in more detail in Parts I.A and I.C.

[4] *See infra* notes 25-27 and accompanying text.

menus.[5] These latter digits are known as "post-cut-through dialed digits" ("PCTDDs").[6]

To date, researchers have failed to develop technology that can effectively screen PCTDDs that contain a telephone user's substantive information, such as account or PIN numbers, from PCTDDs that do not contain substantive information, such as digits the user dials after being connected to a calling card company, which are technically PCTDDs but may also represent the actual destination of the telephone call.[7] Therefore, when using a pen register to collect all digits dialed by a particular telephone user, law enforcement agencies inevitably collect all PCTDDs dialed by the user to navigate automated systems, even when those digits contain the user's substantive information.

Between 2006 and 2008, six courts issued pen register orders denying the government's application to install and use a pen register to collect all PCTDDs dialed by a subject telephone.[8] Principally, this Note extracts from this series of pen register orders the three unique interpretations of the Pen/Trap Statute that informed the courts' conclusions. Next, by analyzing those three perspectives in light of both the statutory text and the legislative history of the Pen/Trap Statute, this Note ultimately argues that the collection of PCTDDs that contain the substantive content of telephone users' communications runs afoul of

---

[5] See *infra* Part I.A. for a more detailed discussion of pen registers. *See also* U.S. Telecom Ass'n. v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000).

[6] *In re* United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking (*S.D. Tex. I*), 441 F. Supp. 2d 816, 818 (S.D. Tex. 2006).

[7] *In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d at 332 n.5; *see also U.S. Telecom*, 227 F.3d at 462 ("Some post-cut-through dialed digits are telephone numbers, such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is 'cut through,' dialing the telephone number of the destination party.").

[8] Each published pen register order denied a law enforcement agency's application to record all digits dialed from a specific telephone using a pen register. *See In re* United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device on Wireless Tele. Bearing Tele. No. [Redacted], Subscribed to [Redacted], Serviced By [Redacted] (*E.D.N.Y. III*), No. 08 MC 0595, 2008 U.S. Dist. LEXIS 101364, at *15-*16 (E.D.N.Y. Dec. 15, 2008); *In re* United States for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices (*E.D.N.Y. II*), No. 08-308, 2008 U.S. Dist. LEXIS 97359, at *26 (E.D.N.Y. Nov. 22, 2008); *In re* United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info. (*S.D. Tex. II*), No. H-07-613, 2007 U.S. Dist. LEXIS 77635, at *34-*35 (S.D. Tex. Oct. 17, 2007); *E.D.N.Y. I*, 515 F. Supp. 2d at 339; *In re* Application of United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking (*S.D. Tex. I*), 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006); *In re* United States for an Order Authorizing the Installation and Use of an Elec. Computerized Data Collection Device Equivalent to a Pen Register and Trap and Trace Device, No. 06:06-mj-1130 (M.D. Fla. June 20, 2006) (order affirming partial denial of application for the installation and use of pen register and trap and trade device). To date, no court has published an order granting such a request, although presumably such orders are granted routinely.

both the Pen/Trap Statute and the Fourth Amendment of the United States Constitution[9] and should be prohibited.

Specifically, in Part I, this Note briefly reviews relevant background information about pen register technology, as well as the common-law and statutory provisions that restrict the use of pen registers and the collection of content by law enforcement agencies. In Part II, this Note emphasizes the interplay between two provisions of the Pen/Trap Statute—18 U.S.C. § 3121(c) and 18 U.S.C. § 3123(7)—which has given rise to the three prominent and conflicting interpretations of the Pen/Trap Statute. By viewing these interpretations in light of traditional canons of statutory interpretation and the statute's legislative history, Part II concludes that the Pen/Trap Statute should not be viewed as authorizing the use of pen registers to collect PCTDDs that contain content. Specifically, because the Fourth Amendment most likely protects PCTDDs that contain content, the canon of constitutional avoidance suggests that future courts should interpret the Pen/Trap Statute to prohibit the collection of PCTDDs that contain content.

Building on Part II's discussion, Part III.A presents this Note's primary conclusion, which is that the statutory ambiguity should be cured by either amending or eliminating 18 U.S.C. § 3121(c). Part III.B briefly summarizes suggestions made by other commentators who have advocated general amendments to the Pen/Trap Statute. Finally, Part IV reemphasizes the conclusion that the collection of content in the form of PCTDDs is unconstitutional and urges Congress to take steps to prevent the continuation of this practice.

I. THE RELATIONSHIP BETWEEN PEN REGISTERS AND THE COLLECTION OF CONTENT

Part I.A explains what a pen register is and traces its evolution from a device that originally assisted telephone service providers in the ordinary course of business, to a tool that law enforcement agencies routinely employ during investigations. Part I.B explores judicial limitations imposed on the government's ability to intercept the content of electronic communications, including its use of pen registers, in a series of Supreme Court decisions. These decisions in turn have informed Congressional action with respect to pen registers, including the original passage of and later amendments to the Pen/Trap Statute, which Part I.C addresses in detail. The brief review of this well-trodden history sets the stage for Part II's analysis of the recent pen register orders and the Pen/Trap Statute's ambiguous text.

---

[9] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

A. Identifying a Pen Register

Telephone service providers use pen registers in the ordinary course of business to perform monthly billing operations and to prevent illegal and fraudulent uses of telephone lines.[10] Yet, as a result of the inherent value of the information that pen registers collect, pen registers are also important for law enforcement agencies conducting investigations into criminal activities.[11] No available statistics tabulate the total number of pen register applications approved in the United States for law enforcement agents.[12] However, one commentator estimated that in 2007 alone, that figure was at least 60,000.[13]

Whether or not a particular device is a pen register depends on the exact capabilities of the device in light of the statutory definition of a pen register.[14] Because technology and statutes constantly evolve, judicial conceptions[15] and statutory definitions[16] of a pen register have also changed over time.[17] The current statutory definition of a pen register contains expansive language that resulted from amendments intended to allow pen registers to monitor activities conducted over a variety of digital mediums, including digital telephones, cellular phones, digital pagers, Internet browsing, and electronic mail.[18] Yet, the earliest

---

[10] United States v. N.Y. Tel. Co., 434 U.S. 159, 174-75 (1977). Providers of electronic or wire communication services may continue to use pen registers in the ordinary course of business as a result of an exception codified in the Pen/Trap Statute. 18 U.S.C. § 3121(b) (2006).

[11] *See N.Y. Tel. Co.*, 434 U.S. at 177-78 (acknowledging congressional intent to treat the pen register as a permissible law enforcement tool); *see also* 86 Ops. Cal. Atty. Gen. 198, No. 03-406 at *2 (Dec. 18, 2003) ("The placement of pen registers and trap and trace devices allows law enforcement officers to obtain such information as the names of suspects in an investigation, the identities and relationship between individuals suspected of engaging in criminal activity, especially in conspiracies, and the location of fugitives.").

[12] Pen registers are approved on an individual basis by courts pursuant to ex parte requests by law enforcement agents. 18 U.S.C. § 3123(a). The Pen/Trap Statute imposes an obligation on the Attorney General to report to Congress each year the total number of pen registers for which agents of the DOJ applied. 18 U.S.C. § 3126. However, these reports are not publicly available and other authors have been unable to obtain them despite thorough efforts. *See, e.g.*, Robert Ditzion, *Electronic Surveillance in The Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1347 n.162 (2004). Most evidence of the total number of pen register applications granted appears to be anecdotal. *See* Giardi, *infra* note 13, at 554; *see also* Carl S. Kaplan, *Concern Over Proposed Changes in Internet Surveillance*, N.Y. TIMES, Sept. 21, 2001, *available at* http://www.nytimes.com/2001/09/21/technology/21CYBERLAW.html/?ex=1236315600&en=c0400d2e20c62f91&ei=5070 (quoting former DOJ trial attorney who claimed to use pen registers to obtain non-content "hundreds of times") (on file with author).

[13] Albert Giardi, Jr., *Companies Caught in the Middle*, *Keynote Address*, 41 U.S.F. L. REV. 535, 554 (2007).

[14] Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 982-86 (1996) (discussing the evolution of the pen register).

[15] *See infra* Part I.B.

[16] *See infra* Part I.C.

[17] *See* Freiwald, *supra* note 14, at 982-86.

[18] *See infra* Part I.C; *see also* 18 U.S.C. § 3127(3) (2006) ("[T]he term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted . . . .").

devices that Congress and courts considered to be pen registers lacked this wide scope of functions.

The primitive pen register of the 1960s attached to a telephone line and then generated a paper tape on which it printed dashes that correlated to the outgoing numbers the user dialed.[19] Because at that time telephone users only used telephones to place phone calls, many believed that any device that detected the digits dialed to connect a call could not reveal the substantive information the user communicated during the call.[20] Understandably, laws and attitudes failed to anticipate how the nature and use of communication devices, including telephones, would evolve and expand in the decades to follow.[21]

Today, telephones serve many purposes aside from facilitating conversation.[22] Similarly, a proliferation of digital devices with complex and innovative capabilities can monitor far more about a single telephone call than merely the digits the user dialed. Devices can easily capture the "time, date, and duration" of calls.[23] In the case of a cellular telephone user, a pen register can supply information that can be used to calculate the user's physical location or track the user's movements in real time.[24] Litigation has tested the outer boundaries of what devices are properly considered to be pen registers. For instance, plaintiffs have challenged the use by law enforcement agencies of pen registers to clone a suspect's pager,[25] track a suspect's web site activity,[26] or monitor the flow of e-mail traffic into and away from a particular e-mail account.[27] In resolving plaintiffs' claims, courts have crafted their views of which devices may qualify as pen registers in light of the statutory text. One court, for instance, speculated that a device that allowed its operator to eavesdrop on actual telephone conversations could fall within the statutory definition of a pen register, so long as the eavesdropping function was

---

[19] *See, e.g.*, United States v. Dote, 371 F.2d 176, 178 (7th Cir. 1966); United States v. Guglielmo, 245 F. Supp. 534, 535 (N.D. Ill. 1965).

[20] United States v. N.Y. Tel. Co., 434 U.S. 159, 166-67 (1977).

[21] *See In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d, 325 328 (E.D.N.Y. 2007). *But see* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) ("Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?").

[22] For instance, the Apple i-Phone allows its user to browse the Internet, e-mail, download music, and utilize maps with GPS tracking, in addition to other features. *See* Apple-iPhone-Features, http://www.apple.com/iphone/features/ (last visited Feb. 9, 2009).

[23] Freiwald, *supra* note 14, at 986.

[24] The use of pen registers to track telephone users in real time is also controversial. *See, e.g.*, Timothy Stapleton, Note, *The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More than the Sum of its Parts?*, 73 BROOK. L. REV. 383, 385 (2007) (recommending that the Pen/Trap Statute be amended to prevent the use of a pen register to collect cell site data without a showing of probable cause).

[25] Brown v. Waddell, 50 F.3d 285, 287 (4th Cir. 1995).

[26] United States v. Forrester, 512 F.3d 500, 504 (9th Cir. 2008).

[27] Warshak v.United States., 532 F.3d 521, 524 (6th Cir. 2008).

inactive.[28] Another court concluded that a device that monitored the URL addresses that the defendant visited, as well as the e-mail addresses of those to whom he sent messages, was a pen register.[29] Recently, another court concluded that a device that collected content was statutorily precluded from being a pen register, even if the government stipulated that it would only decode pre-cut-through dialed digits.[30]

In short, the classification of a device as a pen register is primarily functional, but not exclusively so. The analysis depends not only on the capabilities of a specific device in light of the statutory definition of a pen register, but also turns on the philosophy of the particular court applying that language to a particular device. Accordingly, both Congress and the courts play significant roles in determining whether a device is a pen register.[31] Parts I.B and I.C explore those roles, respectively.

B. The Supreme Court's Treatment of Content, Non-Content, and Pen Registers

The current statutory definition of a pen register provides that the information that a pen register records or decodes "shall not include the contents of any communication."[32] The term "contents"[33] is a legal term of art with a meaning developed over time through both case law and legislation. In simplistic terms, the content of a particular electronic communication includes the substantive aspects of that communication, as distinguished from those attributes of the communication that relate exclusively to its facilitation.[34] The digits dialed to connect a telephone call, the delivery address written on the outside of a mailed envelope,[35] or the email address of the user to whom an email is sent[36] all exemplify attributes that facilitate a communication, but which ordinarily do not reveal the substantive content of the communication.

---

[28] People v. Kramer, 706 N.E.2d 731, 737 (N.Y. 1998) (concluding that if a device's digital and audio functions were "sufficiently discrete" and there was a "remote" likelihood of misuse, the presence of audio-capable technology would not disqualify the device from use as a pen register).

[29] *Forrester*, 512 F.3d at 504.

[30] *In re* United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device on Wireless Tele. Bearing Tele. No. [Redacted], Subscribed to [Redacted], Serviced By [Redacted] (*E.D.N.Y. III*), No. 08 MC 0595, 2008 U.S. Dist. LEXIS 101364, at *8-*9 (E.D.N.Y. Dec. 15, 2008).

[31] *See* Freiwald, *supra* note 14, at 985-86.

[32] 18 U.S.C. § 3127(3) (2006).

[33] *See* 18 U.S.C. § 2510(8) (2006).

[34] Susan Freiwald usefully distinguishes between communication content and communication attributes. *See* Freiwald, *supra* note 14, at 953 ("[A]ttributes [of a communication] include the existence, duration and . . . the identities of the parties to it, their physical locations and their electronic addresses.").

[35] *See, e.g.*, United States v. Huie, 593 F.2d 14, 15 (5th Cir. 1979).

[36] *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

This understanding of content can be traced back to 1967, when the Supreme Court held in *Katz v. United States*[37] that the Fourth Amendment's probable cause requirement applied to the substantive aspects of a telephone communication if the speaker's expectation of privacy in his conversation was reasonable.[38] The Fourth Amendment to the United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[39] In *Katz*, the Court considered whether the government had conducted an unreasonable search by electronically intercepting the dialogue of a telephone call that the defendant placed on a public telephone from within a telephone booth.[40] The Court of Appeals had concluded that the government's action was not a search for Fourth Amendment purposes because the government had not physically entered the telephone booth in order to intercept the communication.[41] The Supreme Court rejected this conclusion, explaining that the Fourth Amendment protects "people—and not simply 'areas' against unreasonable searches and seizures."[42] The Court concluded that to apply the Fourth Amendment more narrowly would be to "ignore the vital role" of the telephone in modern life.[43]

The concurring opinion by Justice Harlan fashioned a two-pronged test to determine whether a search was unreasonable.[44] Courts later adopted this test as the standard for determining the legality of a search under the Fourth Amendment.[45] Under this articulation, the Fourth Amendment protects parties who have either an objectively legitimate expectation of privacy, or a subjective expectation of privacy that "society is prepared to recognize as reasonable."[46] Applying this test to the defendant's conversation in the telephone booth, Justice Harlan concluded that the defendant had a legitimate expectation that what he said to the other party during the call was private.[47] Since his expectation of privacy was reasonable, the interception of the defendant's

---

[37] 389 U.S. 347 (1967).

[38] *Id.* at 353-54.

[39] U.S. CONST. amend. IV.

[40] *Katz*, 389 U.S. at 348-50.

[41] *Id.* at 348-49. This reasoning followed from early Supreme Court jurisprudence. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928) (concluding that warrantless wiretapping was not a search under the Fourth Amendment unless the defendant's physical property had been invaded).

[42] *Katz*, 389 U.S. at 353.

[43] *Id.* at 352.

[44] *Id.* at 361 (Harlan, J., concurring).

[45] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979); *see also* Kyllo v. United States, 533 U.S. 27, 33 (2001) (concluding that the use of thermal imagery to measure heat emanating from within a private home constituted an unreasonable search under the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 213-15 (1986) (concluding that the warrantless observation of a private backyard did not constitute an unreasonable search under the Fourth Amendment).

[46] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (quotation marks omitted).

[47] *See id.*

communication constituted an unreasonable search under the Fourth Amendment.[48]

Congress responded to the *Katz* decision the following year by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[49] which provided statutory protection for the "content"[50] of communications.[51] Part I.C discusses this legislation in greater detail. In short, Title III, commonly known as the "Wiretap Act," set forth procedures for obtaining authorization to intercept a wire or oral communication.[52] Under Title III, after a government agent demonstrates probable cause in a federal court, the court may issue a warrant authorizing the government to intercept the content of a private communication falling under Title III.[53] Title III incorporated the basic principle of *Katz* by defining content, "with respect to any wire, oral or electronic communication, [as] includ[ing] any information concerning the substance, purport or meaning of that communication."[54]

In 1977, in *United States v. New York Telephone Co.*, the Court first considered the relationship between pen registers and the "content" protected by Title III.[55] New York Telephone Company had resisted a directive from the FBI to install pen registers on two telephone lines the defendants used in an illegal gambling enterprise.[56] Although the government possessed probable cause to believe that the defendants used the telephone lines illegally,[57] the telephone company argued that the district court could only order it to furnish facilities and technical assistance to the government in connection with a wiretap order conforming to Title III.[58] The Court rejected this argument and concluded that pen registers were not governed by Title III because they were incapable of "intercept[ing]" the content of wire or oral communications.[59] Relying on the prevalent understanding at the time, the Court concluded that digits dialed into a telephone lacked the capacity to be substantive. Consequently, it followed that pen registers posed a lesser threat to privacy than traditional wiretaps because they

---

[48] *See id.*

[49] 18 U.S.C. §§ 2510-2522 (2006).

[50] *Id.* § 2510(8) (defining "content").

[51] *Id.* § 2511 (prohibiting the interception and disclosure of wire, oral, or electronic communications).

[52] *See id.* §§ 2510-2522.

[53] *Id.* § 2518(1)(a)-(f), (3).

[54] *Id.* § 2510(8).

[55] *See* 434 U.S. 159, 165-68 (1977).

[56] *Id.* at 162.

[57] *Id.* 161-62.

[58] *Id.* at 162-63.

[59] Title III defines "intercept" as the "aural or other acquisition" of content. 18 U.S.C. § 2510(4). Because a pen register does not monitor sound, the court concluded that a pen register cannot "intercept" content. *N.Y. Tel. Co.*, 434 U.S. at 166-67.

could not reveal substantive information about a telephone communication.[60]

In *New York Telephone*, the government possessed probable cause to believe that the defendants used telephone lines illegally.[61] Consequently, the Court had no occasion to rule on the minimal showing of suspicion needed to justify the use of a pen register.[62] However, the Court answered that open question in 1979 in the case of *Smith v. Maryland*.[63] The defendant, Smith, appealed his robbery conviction on the grounds that the government's investigation included the installation and use of a pen register to monitor his telephone use without a warrant.[64] Writing for the Court, Justice Blackmun affirmed the decision by the Court of Appeals of Maryland,[65] and held that Fourth Amendment protections do not apply to dialed digits.[66] To reach this conclusion, the Court applied the *Katz* test and concluded that a telephone user does not have a legitimate expectation of privacy in dialed numbers because the user is aware that the telephone company monitors the numbers dialed to connect a telephone call.[67] This holding reflected a basic tenet of the Court's Fourth Amendment jurisprudence: an individual does not have a reasonable expectation of privacy in information that the individual voluntarily turns over or conveys[68] to a third party.[69] In revealing information to a third party, even on the assumption that it will be kept secret, one assumes the risk that that party may reveal that information to the government.[70]

The Court identified several ways in which a telephone subscriber receives notice that a telephone company has facilities that enable it to document its subscribers' dialing activities.[71] The Court

---

[60] *See id.* at 168.

[61] *Id.* at 162.

[62] *See id.* at 165 n.7.

[63] 442 U.S. 735 (1979).

[64] *Id.* at 737.

[65] Smith v. Maryland, 389 A.2d 858 (1978).

[66] *Smith*, 442 U.S. at 742.

[67] *Id*.

[68] *See id*.

[69] *Id.* at 743-44. Professor Orin S. Kerr refers to this principle as "the disclosure principle." Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 628 (2003); *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009) (defending "the controversial rule that information loses Fourth Amendment protection when it is knowingly revealed to a third party"). The disclosure principle has guided judicial decision making in a variety of contexts. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442 (1976) (bank depositor's records, including checks and deposit slips); United States v. Huie, 593 F.2d 14, 15 (5th Cir. 1979) (address information on outside of mailed envelope); Tyler v. Berodt, 877 F.2d 705, 706-07 (8th Cir. 1989) (interception of content of telephone conversation on portable phone by radio in the vicinity).

[70] *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 442); *see also* United States v. Jacobsen, 466 U.S. 109, 117 (1984) (discussing the disclosure principle in connection with the seizure and search by federal agents of packages determined to contain cocaine).

[71] A telephone user realizes that by dialing digits, those digits are conveyed to the telephone company in order to complete the call. The user also receives a monthly itemized bill that

emphasized that its conclusion did not rely on whether the telephone company in fact monitored any dialed digits, but rather rested on the petitioner's knowledge that such a possibility existed.[72] Because a telephone user has notice of the possibility of monitoring, the use of a telephone constitutes an assumption of risk by the user that digits dialed will not be secret from the telephone company, which might in turn reveal those numbers to the government.[73] Even if an individual telephone user subjectively believed that dialed digits were private, that belief would be unreasonable and, under *Katz*, not protected by the Fourth Amendment.[74] Thus, the Court held that "[t]he installation and use of a pen register . . . was not a search, and no warrant was required."[75]

Smith marked the last time that the Supreme Court considered the use of pen registers. Therefore, *Smith*'s holding—that the use of a pen register does not constitute a search and therefore does not require probable cause—remains relevant to that area of law today.[76] However, as the next subsection addresses, Congress has acted on several occasions since *Smith* to craft and amend federal law in order to keep pace with evolving technology and the specific questions raised by the continued exception of pen registers from Title III's warrant requirement.

C. The Evolution of the Pen/Trap Statute

The statutory scheme that regulates the use of pen registers can best be understood by examining in chronological order four public laws, including Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[77] the Electronic Communications Protection Act of 1986 ("ECPA"),[78] the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"),[79] and the USA PATRIOT Act of 2001,[80] each

---

lists numbers dialed. Most telephone books also notify telephone users that the telephone company may monitor dialing activity to identify users that make improper phone calls, or to regulate or maintain the telephone line. Thus, a telephone user is on notice of the company's ability to monitor dialed digits. *Smith*, 442 U.S. at 742-43. Today, these uses are statutorily preserved by an exception in 18 U.S.C. § 3121(b) (2006).

[72] *See Smith*, 442 U.S. at 745.

[73] *Id.* at 743.

[74] *Id.* at 743-44. The court noted, however, that its conclusions applied as a result of the telephone company's known practices, and therefore did not foreclose the reasonableness of the defendant's expectation that the content of his telephone conversation would remain private. *See id.* at 743.

[75] *Id.* at 745-46 (quotation marks omitted).

[76] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 509 (9th Cir. 2008) (considering the application of *Smith* to the use of pen registers to record e-mail and Internet activities).

[77] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2006)).

[78] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522, 3121-3127 (2006) and in scattered sections of 18 U.S.C.).

[79] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010 (2006) and in scattered sections of 18 U.S.C.).

of which directly affected the use of pen registers. This Note takes the view that legislative history, particularly statements in committee reports or made by a bill's sponsor, is relevant to courts that must apply a statute that, by its plain language, is ambiguous.[81] The extent to which this sort of evidence should influence judicial decision making is often challenged by textualists, who take the view that the "text is the law."[82] Nevertheless, relevant examples of legislative history are interwoven with the history that this Part presents.

The evolution of the statutory scheme that regulates electronic surveillance, including the use of pen registers, has been fueled by Congress' consistent desire to keep pace with the challenges posed by emerging technologies to traditional notions of privacy.[83] By enacting Title III in 1968, Congress took a major step forward in its effort to protect electronic communications.[84] The purpose of that bill was to become "the primary law protecting the security and privacy of business and personal communications."[85] However, Title III only provided protection for "oral" or "wire" communications that could "be overheard and understood by the human ear,"[86] and which were transmitted over "common carriers."[87]

This changed in 1986 with the passage of the Electronic Communications Protection Act.[88] The ECPA amended Title III to extend its protections to new forms of electronic communications.[89] Members of Congress had become aware of dramatic technological changes that created new risks to the privacy and security of transmitted communications.[90] The ECPA sought to prevent unauthorized interceptions of many different electronic communications in the same

---

[80] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of U.S.C.).

[81] *See, e.g.*, Blanchard v. Bergeron, 489 U.S. 87, 91-96 (1989) (incorporating Senate and House Committee reports to interpret an ambiguous provision of law).

[82] ANTONIN SCALIA, A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW 22-25 (1997) (presenting "textualist" philosophy of legal interpretation); *see also Blanchard*, 489 U.S. at 97-98 (Scalia, J., concurring) (disagreeing with the majority's decision to incorporate Senate and House Committee reports to interpret an ambiguous provision of law).

[83] As one court noted, this "history reflects persistent Congressional efforts to assure that communications contents retain their protected legal status in the face of changing technology and law enforcement capabilities." *S.D. Tex. I*, 441 F. Supp. 2d at 826.

[84] 18 U.S.C. §§ 2510-2522 (2006).

[85] S. REP. No. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556; *see also* Gelbard v. United States, 408 U.S. 41, 46 (1972).

[86] S. REP. No. 99-541, at 2, *as reprinted in* 1986 U.S.C.C.A.N. at 3556; *see also* 18 U.S.C. §§ 2510(1)-(2), 2511.

[87] S. REP. No. 99-541, at 2, *as reprinted in* 1986 U.S.C.C.A.N. at 3556.

[88] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522, 3121-3127 (2006) and in scattered sections of 18 U.S.C.).

[89] Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995).

[90] *See* S. REP. No. 99-541, at 2, *as reprinted in* 1986 U.S.C.C.A.N. at 3556 (discussing new forms of technology); *see also Brown*, 50 F.3d at 289 (reviewing the legislative history of the passage of the ECPA).

way that Title III had done for oral and wire communications.[91] The ECPA defined an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[92] This broad definition brought modern technologies, such as the Internet and e-mail, under Title III's purview. Consequently, law enforcement agencies had to follow Title III's procedures, including a showing of probable cause,[93] in order to intercept the content of any electronic communication.

The ECPA also articulated federal guidelines for the installation and use of pen registers.[94] In 1986, Congress viewed a pen register as a device that, in its limited capacity, could only record the telephone numbers to which a telephone user placed calls, yet could not capture any part of an actual telephone conversation.[95] Consequently, the ECPA established separate[96] and lower[97] standards for the installation and use of pen registers than those that applied to content-intercepting devices under Title III. The distinct sections of the ECPA that regulate pen registers and trap-and-trace devices are referred to as the Pen/Trap Statute.[98]

The standards that govern the installation and use of a pen register under the Pen/Trap Statute differ from those that govern content-intercepting devices under Title III in four ways that are relevant to this discussion generally, as well as to the statutory amendments that Part III of this Note suggests.

First, Title III applications must satisfy a higher standard of proof than pen register applications.[99] Under 18 U.S.C. § 2518, a judge may only issue a wiretap warrant under Title III if the judge determines on the basis of the facts submitted by the applicant that there is probable cause to believe that "an individual is committing, has committed, or is

---

[91] *Brown*, 50 F.3d at 289.

[92] 18 U.S.C § 2510(12) (2006).

[93] *See id.* § 2518(1)(d), (3).

[94] *See id.* §§ 3121-3127 (2006).

[95] S. REP. No. 99-541, at 10, *as reprinted in* 1986 U.S.C.C.A.N. at 3564.

[96] *See* 18 U.S.C. § 2511(2)(h)(i) (providing that the use of pen registers is not regulated by Title III).

[97] *See infra* note 102 and accompanying text.

[98] *See* 18 U.S.C. §§ 3121-3127. The name "Pen/Trap Statute" derives from its dual application to both pen registers and trap-and-trace devices. *See* DIFFIE & LANDAU, *supra* note 2, at 117.

[99] *Compare* 18 U.S.C. § 2518(1) (requiring extensive disclosure incident to a wiretap application including, among other things, full and complete statements of fact about the investigation and any alternative procedures employed to obtain the desired information without a wiretap), *with id.* § 3122(b) (requiring minimal disclosure incident to a pen register application, limited to the identity of the applicant and the agency conducting the investigation and a certification that the information sought is relevant to the investigation being conducted).

about to commit" a qualified offense.[100] In contrast, a pen register application requires only that an attorney for the government certify to the court in writing and under oath that "the information likely to be obtained [by a pen register] is relevant to an ongoing criminal investigation being conducted" by the official's agency.[101] The lower standard of proof required for pen register applications is "far from burdensome."[102]

Second, if an attorney for the government or a law enforcement official has made the proper certification to the court, then the court is compelled to order the installation and use of a pen register.[103] This compulsory order leaves no room for judicial discretion in determining whether or not a pen register should be issued. A wiretap application, in contrast, is permissive. A federal judge has wide latitude for factual review in determining whether the particular facts support authorizing the interception of content.[104]

Third, the Pen/Trap Statute does not contain an exclusion requirement. As a result of this omission, evidence obtained pursuant to the wrongful or unlawful installation or use of a pen register may be admitted as evidence in a criminal case.[105] The statute penalizes a knowing wrongdoer by authorizing the imposition by the court of either a fine or prison sentence, yet it has no effect on the fruit of such wrongdoing.[106] This stands in contrast to the treatment of content wrongfully intercepted pursuant to Title III, which may be suppressed upon a petitioner's motion.[107]

---

[100] *Id.* § 2518(3)(a).

[101] *Id.* § 3122(b).

[102] *In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 329 (E.D.N.Y. 2007); *see also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 48 (2004); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1566-67 (2004) (discussing the low standard of proof for a pen register application).

[103] 18 U.S.C. § 3123(a)(1)-(2); *see also* S. REP. No. 99-541, at 47 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3601 ("[Section 3123(a)] does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted."); 147 CONG. REC. S10,990, S11,000 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) ("The court is required to issue an order upon seeing the prosecutor's certification. The court is not authorized to look behind the certification to evaluate the judgment of the prosecutor.").

[104] 18 U.S.C. § 2518(3) (providing that upon a satisfactory Title III application, a judge *may* enter a wiretap order) (emphasis added); *see also* United States v. Diaz, 176 F.3d 52, 110 (2d Cir. 1999) (discussing the circumstances under which a federal judge may authorize a wiretap order).

[105] *See, e.g.*, United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995); *see also* United States v. Thompson, 936 F.2d 1249, 1251-52 (11th Cir. 1991) (concluding that defendant could not show that Congress intended, either explicitly or implicitly, to provide suppression as a remedy for violation of the Pen/Trap Statute).

[106] 18 U.S.C. § 3121(d).

[107] *See id.* § 2518(10)(a) (providing aggrieved party the right to move to suppress the fruits gathered pursuant to wiretap authorization that was unlawful due to either procedural or substantive misuse).

Fourth, Title III contains a minimization requirement.[108] Under 18 U.S.C. § 2518(5), even where the government intercepts communications pursuant to a valid wiretap order, it must "minimize the interception" of irrelevant communications.[109] Courts view this provision as requiring agents to take reasonable steps to avoid recording the content of communications that are not relevant to their investigations.[110] At the time of the ECPA's passage, however, no such provision was incorporated into the Pen/Trap Statute.[111] This omission may have been sensible given the fact that in 1986, neither courts nor Congress anticipated that the collection of dialed digits by a pen register could reveal more than the telephone number of the party to whom a call had been directed, which, under *Smith*, was not protected information.[112]

By 1994, however, this view had changed markedly. That year, Congress passed CALEA[113] in response to new challenges faced by law enforcement as a result of the "explosive growth" of wireless services and technologies, such as call forwarding, that had started to impede the government's traditional wiretapping abilities.[114] CALEA required the telecommunications network providers to develop the capacity to self-monitor their networks in order to expedite compliance with wiretap, pen register, or other court orders for electronic information.[115] While expanding government access to electronic information, Congress also struggled to protect the reasonable expectation of privacy the law accorded to the content of electronic communications.[116]

Section 207 of CALEA enacted 18 U.S.C. § 3121(c). Entitled "Limitation," this section amended the Pen/Trap Statute by imposing a minimization requirement on the use of pen registers.[117] Under the limitation, any agency authorized to install a pen register "shall use technology reasonably available to it that restricts the recording or

---

[108] *See id.* § 2518(5).

[109] *Id.*

[110] *See, e.g.*, Scott v. United States, 436 U.S. 128, 140 (1978).

[111] 18 U.S.C. §§ 3121-3127.

[112] *S.D. Tex. I*, 441 F. Supp. 2d 816, 826 (S.D. Tex. 2006); *see also supra* notes 75-76 and accompanying text.

[113] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010 (2006) and in scattered sections of 18 U.S.C.).

[114] H.R. REP. No. 103-827, at 9, 12 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3489, 3492; *see also* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) (summarizing purposes of CALEA, including impediments posed to law enforcement by advanced technologies).

[115] *See* H.R. REP. No. 103-827, at 9-10, *as reprinted in* 1994 U.S.C.C.A.N. at 3489-90.

[116] *Id.* at 13 *as reprinted in* 1994 U.S.C.C.A.N. at 3493 ("[CALEA] seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."); *see also* 47 U.S.C. § 1002(a)(4)(A) (2006) (emphasizing the importance of monitoring telecommunications networks "in a manner that protects . . . the privacy and security of communications and call-identifying information not authorized to be intercepted").

[117] Pub. L. No. § 207, 108 Stat. 4292 (codified as amended at 18 U.S.C. § 3121(c) (2006)).

decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications."[118] This new language reflected an emerging awareness of the fact that the digits a pen register collected could include content.[119]

Divining the exact purpose behind the addition of the limitation, however, is no simple task.[120] Statements of purpose in the House Report[121] and statements by the bill's sponsor, Senator Patrick Leahy,[122] indicate that Congress intended the limitation to protect the exercise of the government's surveillance authority and may have contemplated allowing the government to collect PCTDDs that included content, so long as it endeavored to minimize content by using reasonably available technology.[123] On the other hand, statements of purpose[124] and statements

---

[118] 18 U.S.C. § 3121(c) (2006).

[119] During hearings in March, 1994, Senator Leahy and then FBI Director Louis Freeh discussed the fact that some PCTDDs contained content:

> Sen. LEAHY: You say this proposal would not expand law enforcement's authority to collect data on people, and yet if new technologies are used where we can dial up everything from a video movie to doing our banking over the phone, you are going to have access to a lot more data, just because the phone is being used.
>
> Mr. FREEH: I do not want that access, and I am willing to concede that. What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I have now under pen register authority. As to the banking accounts and what movies somebody is ordering at Blockbuster, I do not want it, do not need it, and I am willing to have technological blocks with respect to that information, which I can get with subpoenas or another process. I do not want that in terms of my access, and that is not the transactional data that I need.

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings Before the Subcomm. on Technology and the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary, 103d Cong. 50 (1994) (statements of Sen. Leahy and Louis J. Freeh, Director, Fed. Bureau of Investigation) [hereinafter Freeh Statement].

[120] *See infra* Part II.C.

[121] H.R. REP. No. 103-827, at 17, *as reprinted in* 1994 U.S.C.C.A.N. at 3497 ("[T]he bill . . . [e]xpressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number . . . . Further, the bill requires law enforcement to use reasonably available technology *to minimize* information obtained through pen registers.") (emphasis added).

[122] 140 CONG. REC. S11,055, S11,055-56, S11,059 (daily ed. Aug. 9, 1994) ("[The limitation requires that a] government agency authorized to install and use a pen register under this chapter or under State law, shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."); *In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 333 (E.D.N.Y. 2007) (citation omitted).

[123] *See E.D.N.Y. I*, 515 F. Supp. 2d 325, 333 (E.D.N.Y. 2007) (noting comments by Sen. Leahy in support of both interpretations of the 1994 amendments).

[124] *See* S. REP. No. 103-402, at 10 (1994) ("The bill further protects privacy by requiring telecommunications systems to protect communications not authorized to be intercepted and by restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information.").

by Senator Leahy[125] in the Senate Report indicate that Congress intended the limitation to restrict the government's access to transactional information, but are not amenable to an interpretation that views minimization favorably.

As Congress prepared to pass the USA PATRIOT Act of 2001 seven years later, Senator Leahy made several statements that appeared to support the view that he believed that Congress intended the limitation to prevent the collection of content.[126] That year, Congress considered two proposed amendments to the Pen/Trap Statute, each of which prohibited the use of a pen register to collect content.[127] To illuminate the necessity of the proposed amendments, Senator Leahy explained that although he had added the 1994 limitation after he "recognized that [pen registers] collected content and that such collection was unconstitutional on the mere relevance standard,"[128] information obtained from the F.B.I. in June 2000 indicated that the limitation had not deterred law enforcement officials from collecting content with pen registers.[129] The limitation did not have the effect of prohibiting the collection of content since, as the government argued, no technology was reasonably available that would allow it to distinguish PCTDDs that contained content from those that did not.[130] Because it did not interpret the limitation's prohibition to be absolute, the government had continued to collect content with pen registers in the same way that it had done for years.[131]

In this context, Congress passed the PATRIOT Act, which, pursuant to § 216, amended two sections of the Pen/Trap Statute.[132] First, § 216(a) amended 18 U.S.C. § 3121(c)—the 1994 limitation—to prohibit the collection of content pursuant to the installation and use of a pen register. As a result, the text of 18 U.S.C. § 3121(c) read and continues to read:

> A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic

---

[125] *See* 140 CONG. REC. at S11,056 (statements of Sen. Leahy); 140 CONG. REC. S14,732, S14,732 (daily ed. Oct. 7, 1994) (statements of Sen. Leahy in support of Edwards-Leahy Digital Telephony bill).

[126] *See* 147 CONG. REC. S10,990, S11,000 (daily ed. Oct. 25, 2001) (statements of Sen. Leahy). *But see infra* Part II.C.

[127] USA PATRIOT Act, Pub. L. No. 107-56, § 216, 115 Stat. 288, 290 (codified as amended at 18 U.S.C. §§ 3121(c), 3127(3)-(4) (2006)).

[128] 147 CONG. REC. at S11,000 (statements of Sen. Leahy).

[129] *Id.* ("[T]he FBI advised me in June 2000, that pen register devices for telephone services 'continue to operate as they have for decades' and that 'there has been no change . . . that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.'" (quoting FBI's explanation to Senator Leahy)).

[130] *See id.* For a summary of this same history, see Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1198 (2004).

[131] 147 CONG. REC. at S11,000 (statements of Sen. Leahy).

[132] *See* Pub. L. No. 107-56, § 216, 115 Stat. 272, 288, 290 (2001) (codified as amended at 18 U.S.C. §§ 3121(c), 3127(3)-(4)(2006)).

> or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications *so as not to include the contents of any wire or electronic communications*.[133]

Section 216(c)(2) also modified 18 U.S.C. § 3127(3), which contains the statutory definition of a pen register.[134] Specifically, Congress defined a pen register, for the first time, as a device that cannot collect content. The definition read and continues to read:

> [T]he term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information *shall not include the contents of any communication* . . . .[135]

From this history, it is evident that when the 2001 amendments to the Pen/Trap Statute took effect, Congress was aware that PCTDDs could contain content. Further, Congress recognized that the government had interpreted the limitation that CALEA imposed in 1994 to authorize the collection of all PCTDDs in the absence of reasonably available technology to sort content from non-content. While amending the Pen/Trap Statute to include new prohibitions on content collection, Congress did not eliminate the "reasonably available technology" clause, which formed the basis of the government's claimed authority to collect all PCTDDs. These observations are relevant to the analysis of the Pen/Trap Statute that courts have performed, which is discussed in Part II.

II. INTERPRETING THE PEN/TRAP STATUTE

Until 2006, no court directly addressed the question of whether the Pen/Trap Statute authorizes law enforcement agencies to collect PCTDDs that contain content.[136] Between 2006 and 2008, six courts[137] issued written orders that justified their decisions to deny the portion of a law enforcement agent's ex parte application that sought to collect all

---

[133] 18 U.S.C. § 3121(c) (2006) (emphasis added to reflect the 2001 amendment).

[134] *Id.* § 3127(3).

[135] *Id.* (emphasis added to reflect the 2001 amendment). The definition continues, "such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business." *Id.* The PATRIOT Act also amended 18 U.S.C. § 3127(4), which defines trap and trace devices, to provide that a trap and trace device shall not collect the content of a communication. PATRIOT Act § 216(c)(3).

[136] During this time, two courts referenced the PCTDD question in dicta. *See* U.S. Telecom Ass'n v. FCC, 277 F. 3d 450, 462 (D.C. Cir. 2000); *see also In Re* United States for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 48 (D. Mass. 2005).

[137] *See supra* note 8.

dialed digits from a telephone pursuant to the Pen/Trap Statute.[138] Given the ex parte nature of each proceeding, the courts solicited amicus briefs to represent the interests of the telephone user. The six decisions reached inconsistent conclusions about whether the Pen/Trap Statute is ambiguous, whether canons of statutory interpretation are relevant to the question and, if so, how they apply, whether legislative history helps to answer the question, and whether the Fourth Amendment protects PCTDDs that contain content.

This Part approaches each question in turn. After identifying the different ways that the statute can be interpreted, Part II.A concludes that the plain language of the Pen/Trap Statute does not overwhelmingly lend support to any particular textual interpretation. As a result of this ambiguity, Part II.B applies traditional canons of statutory interpretation to the different interpretations of the Pen/Trap Statute. Although the canons lend support to the position that the Pen/Trap Statute does not authorize the collection of content, they ultimately fail to be entirely persuasive. Part II.C concludes that the legislative history of the Pen/Trap Statute is also not dispositive on the question of whether the statute authorizes the collection of minimal PCTDD content. However, Part II.D concludes that because society is prepared to recognize a reasonable expectation of privacy in PCTDDs that contain content, the canon of constitutional avoidance counsels against an interpretation that the Pen/Trap Statute authorizes the collection of content using a pen register.

A. The Plain Language of the Pen/Trap Statute

Following the cardinal rule of statutory interpretation, the opposing parties have argued that the plain language of the Pen/Trap Statute mandates a particular conclusion about the legality of collecting PCTDDs that contain content with a pen register.[139] Consequently, three primary interpretations of the text have arisen, each of which fundamentally conflicts with the others. The role of the court in such circumstances is to determine whether the statute's plain language supports one of the interpretations.[140] This Part briefly summarizes the

---

[138] That no court addressed this issue until five years after the passage of the PATRIOT Act may be partially attributed to the fact that pen register applications are ex parte proceedings that do not usually result in the publication of a written decision. 18 U.S.C. § 3123(a)(1) (2006). Further, because the court is not entitled to receive facts concerning the investigation beyond the investigator's stipulation that the information sought to be collected is relevant, 18 U.S.C. § 3122(b) (2006), little has been documented about the number of pen register applications made and granted each year, or about the reasons that a particular court granted or denied an application. *See, e.g.*, Ditzion, *supra* note 12, and accompanying text; *see also* Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 589-90 (2007).

[139] *See e.g.*, TRW Inc. v. Andrews, 534 U.S. 19, 31 (2001); Duncan v. Walker, 533 U.S. 167, 174 (2001).

[140] *See e.g.*, Barnhart v. Sigmon Coal Co., 534 U.S. 438, 450 (2002).

three perspectives in order to illustrate that the Pen/Trap Statute is ambiguous. Next, Part II.B critiques each perspective using traditional canons of statutory interpretation.

1. The Government's Theory

The government has argued that the Pen/Trap Statute's text authorizes the collection of PCTDDs that contain content.[141] The government's briefs express this theory in two assertions. First, the limitation in 18 U.S.C. § 3121(c) requires that if technology that can distinguish between content and non-content is reasonably available, then the government must use that technology to avoid collecting content.[142] However, if technology that can screen content from non-content is not reasonably available, then the limitation permits the pen register to access content incident to its collection of non-content.[143] Accordingly, the government views the limitation as an exception[144] to the language in 18 U.S.C. § 3127(3) that provides that a pen register shall not collect the content of any communication.[145]

2. The "Added Precaution" Theory

A contrary perspective adopted by some courts is that the limitation does not operate as an exception to the general prohibition on collecting content, but rather precludes the collection of all PCTDDs where the collection of content cannot be prevented.[146] This theory can also be reduced to two assertions. First, if technology that is reasonably available to minimize the collection of content exists, then the

---

[141] The government articulated this interpretation in 2002, shortly after the PATRIOT Act went into effect. Memorandum from Larry D. Thompson, Deputy U.S. Att'y Gen., to Ass't U.S. Att'y Gen., Criminal Div., et al., Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices 3-4 (May 24, 2002) [hereinafter Thompson Memo]. This interpretation continues to represent the government's position on the issue. *See, e.g.*, Government's Supp. Memo. of Law Demonstrating that Incidental Access to Post-cut-through Dialed Digit Content Under the Pen/Trap Statute Is Constitutional at 1-2, *In re* United States for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Services and (2) Authorizing Release of Subscriber Information, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (No. 06 Misc. 547, 06 Misc. 561, 07 Misc. 120), 2007 U.S. Dist. Ct. Br. LEXIS 541 at *1-*2 [hereinafter Gov't Brief, June '07].

[142] Thompson Memo, *supra* note 141, at 4 (articulating the DOJ's position that the inadvertent collection of PCTDDs that contain content should be avoided but, where it occurs, the agent should not use the content affirmatively); *see also* Gov't Brief, June '07, *supra* note 141, at *1-*2.

[143] Gov't Brief, June '07, *supra* note 141, at *11.

[144] *Id.* ("The [limitation] establishes ground rules governing circumstances in which it is difficult for the government to know in advance" whether pen register information represents content or non-content.).

[145] 18 U.S.C. § 3127(3) (2006).

[146] *In re* Application of United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Consumer Records, and (3) Cell Phone Tracking (*S.D. Tex. I*), 441 F. Supp. 2d 816, 824-25 (S.D. Tex. 2006).

government must use it.[147] However, if no technology that is reasonably available can separate content from non-content, then the government may not collect PCTDDs.[148] Under this theory, the limitation is only operative when technology that can screen content from non-content is reasonably available, in which instance the government must use it. Where such technology is not reasonably available, the limitation does not otherwise condone the use of a pen register to collect content.[149] Thus, the limitation functions primarily as an "added precaution" to prevent content collection.[150]

3. The "Preclusive Definition" Theory

A third perspective adopted by one court is similar to the second. Its proponents emphasize that under the definition of a pen register in 18 U.S.C. § 3127(3), it is unlawful for a pen register to record the content of a communication.[151] If a device records PCTDDs that contain content, then that device is not a pen register.[152] Under this theory, the limitation provision is not a factor in the analysis of whether in certain circumstances a pen register can collect PCTDDs that contain content, because as soon as a device collects content, the device is not a pen register, and the Pen/Trap Statute is no longer implicated.[153]

4. Statutory Ambiguity

The next subsection demonstrates problems with each of these interpretations.[154] At this point, it is only necessary to observe that each perspective is based on and equally supported by the plain language of the Pen/Trap Statute. This illuminates the fundamental flaw of the statute: it provides no guidance about the effect of an absence of reasonably available technology to effectively filter content from non-content. A more sensible approach is to view the first three theories

---

147 *Id.* at 825.

148 *Id*. at 825-26.

149 *Id*.; *see also* United States for an Order Authorizing the Installation and Use of an Elec. Computerized Data Collection Device Equivalent to a Pen Register and Trap and Trace Device, No. 06:06-mj-1130 at 5 (M.D. Fla. June 20, 2006) ("In the Court's view, § 3121(c) operates as an additional privacy safeguard, rather than an enabling provision.").

150 *In re* United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trade Device, and (2) Authorizing Release of Subscriber and Other Info. (*S.D. Tex. II*), 2007 U.S. Dist. LEXIS 77635 at *31-32 (S.D. Tex. Oct. 17, 2007) ("The requirement to use 'reasonably available technology' is a supplement to the Government's obligation not to collect contents with a pen register.").

151 *In re* United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device on Wireless Tele. Bearing Tele. No. [Redacted], Subscribed to [Redacted], Serviced By [Redacted] (*E.D.N.Y. III*), 2008 U.S. Dist. LEXIS 101364 at *8-*9 (E.D.N.Y Dec. 15, 2008).

152 *Id.* at *8-*9, *11.

153 *See id.* (denying government's pen register application with no discussion of 18 U.S.C. § 3121(c)).

154 *See infra* Part II.B.

critically and conclude, as one court has done, that the Pen/Trap Statute is ambiguous.[155] The language of the statute contradicts itself because the definition of a pen register includes an unconditional prohibition of the use of a pen register to collect content,[156] yet the limitation provision appears to require only the use of reasonably available technology to prevent the collection of content.[157]

B. Applying Canons of Statutory Interpretation to the Pen/Trap Statute

Canons of statutory interpretation are "rules of thumb" that courts apply to aid in statutory interpretation.[158] Courts are not bound by the result that the application of a particular canon would produce.[159] Further, the individual canons have been criticized for being easily countered.[160] Nevertheless, courts continue to apply them routinely. Because the ambiguity inherent in the Pen/Trap Statute gives rise to several possible interpretations of its text, this Part will assess the effect of several applicable canons of construction on the three emergent interpretations.

The government's interpretative theory[161] is undesirable because it interprets statutory silence as modifying the plain commandment of 18 U.S.C. § 3127(3) that a pen register shall not collect content.[162] To subscribe to the government's view is to conclude that the limitation, which is only operative after the government has received authorization to use a pen register, alters the scope of what a pen register can do.[163] Yet, the only way to reach the conclusion that the limitation alters the definition of a pen register is to rely on Congressional silence, which is generally undesirable.[164] The statute fails to provide that the lack of reasonably available technology to sort content from non-content has any effect on the abilities of a pen register. This silence should not be interpreted as an implied exception to the clear commandment of 18

---

[155] *In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 332 (E.D.N.Y. 2007).

[156] *Id.*

[157] *Id*.

[158] Connecticut Nat. Bank v. Germain, 503 U.S. 249, 253 (1992).

[159] WILLIAM N. ESKRIDGE, JR., PHILIP P. FRICKEY & ELIZABETH GARRETT, CASES AND MATERIALS ON LEGISLATION STATUTES AND THE CREATION OF PUBLIC POLICY 849 (4th Ed. 2007).

[160] *See generally* Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are to Be Construed*, 3 VAND. L. REV. 395 (1950).

[161] *See supra* notes 141-145.

[162] This canon of interpretation may be referred to as the "dog that did not bark." Chisom v. Roemer, 501 U.S. 380, 396 n.23 (1991); *see also* Zuni Pub. Sch. Dist. No. 89 v. Dept. of Educ., 127 S. Ct. 1534, 1541-45 (2007).

[163] *S.D. Tex. I*, 441 F. Supp. 2d 816, 824 (S.D. Tex. 2006).

[164] *See Chisom*, 501 U.S. at 396.

U.S.C. § 3127(3), since it can be presumed that if Congress intended such an exception, it could easily have provided it explicitly.[165]

A second canon of interpretation advises courts to interpret an ambiguous statutory provision in a way that is consistent with the whole act of which it is a part.[166] Under this canon, viewing the limitation as a prohibition of the collection of content where sorting technology is not reasonably available—the added precaution theory that some courts have adopted—is preferable to the government's theory. Such an interpretation has the advantage of maintaining consistency within the Pen/Trap Statute, since it does not require inferring from statutory silence exceptions to the plain commandment in 18 U.S.C. § 3127(3).[167] In this way, the interpretation minimizes the conflict between the limitation and the definition.

On the other hand, the precaution theory can be criticized on the grounds that adopting it renders the limitation mere surplusage. A separate canon of construction guides courts to avoid such a result, counseling against interpretations of statutory provisions that strip particular words of meaning.[168] To conclude, as the precaution theory does, that the limitation operates to "supplement"[169] the definition of a pen register is to say that the limitation merely reiterates, or repeats, what is written elsewhere. Yet such repetition is redundant. If a pen register by definition cannot collect content, then the limitation is unnecessary to the extent that it merely functions to remind courts that a pen register cannot collect content.

Formal logic is a useful way of illustrating the application of the canons of interpretation to the government's theory and the precaution theory.[170] As noted above, each perspective imposes a "gloss"[171] onto the interplay between the two statutory provisions. Although the statute is not phrased in the form of an if-then conditional, both perspectives proceed from the assumption that it can be understood as such.[172] For instance, both theories concur that under the statute, if technology to sort content from non-content is reasonably available, then the government must use it to prevent the collection of content (if X, then Y).[173] Yet the

---

[165] *See, e.g.*, Landgraf v. USI Film Prods., 511 U.S. 244, 259-60 (1994).

[166] *See, e.g.*, Gonzales v. Oregon, 546 U.S. 243, 273-74 (2006).

[167] FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000).

[168] Circuit City Stores v. Adams, 532 U.S. 105, 113-14 (2001); *see e.g.*, TRW Inc. v. Andrews, 534 U.S. 19, 31 (2001).

[169] *See supra* note 150 and accompanying text.

[170] This method of analysis comes from an amicus brief submitted by the Federal Defenders of New York. Supplemental Memorandum of Law by Amici Curiae for Fed. Defenders of N.Y., Inc. & Elec. Frontier Found. at 33-34, *In re* Orders (1) Authorizing Use of Pen Registers and Trap and Trace Services and (2) Authorizing Release of Subscriber Information, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (No. 06-Misc.-547, 561), 2007 U.S. Dist. Ct. Br. LEXIS 540, at *33-*34 [hereinafter Supp. Amicus Brief, July '07].

[171] *See S.D. Tex. I*, 441 F. Supp. 2d 816, 824-25 (S.D. Tex. 2006).

[172] *See supra* notes 142-143, 147-148 and accompanying text.

[173] Supp. Amicus Brief, July '07, *supra* note 170, at *33-*34.

two perspectives diverge with respect to the consequences that arise if no technology is reasonably available to perform the sorting (not X). The government's theory concludes that if no technology exists, the government can collect content (if not X, then not Y). The precaution theory concludes that if no technology exists, the government cannot collect content (if not X, then Y). Yet both perspectives suffer from a logical fallacy.

By concluding that if not X, then not Y, the government's perspective commits the common logical error of denying the antecedent.[174] In an if-then conditional such as "if X then Y," the negation of X has no bearing on whether or not Y obtains.[175] It follows that in the Pen/Trap Statute, even if it is correct to reduce the statute to a conditional form, the absence of reasonably available technology (not X) does not require any particular result as to whether or not a pen register can collect content (maybe Y, but maybe not).

Similarly, under the precaution approach (if not X, then Y), X is stripped of any utility because Y remains constant whether or not the condition X is satisfied. Proponents of this theory argue that if technology is reasonably available (if X), then no content may be collected (then Y). But the same proponents also argue that if technology is not reasonably available (if not X), then no content may be collected (then Y).[176] Because content may not be collected whether or not technology is reasonably available, it appears that there is no relationship between X and Y. This, in turn, reiterates the conclusion that under the precaution theory, the limitation is superfluous.

The definitional theory conflicts even more clearly with the canon against superfluities.[177] As noted above, under the definitional theory, the limitation does not factor into the analysis of a pen register's ability to collect content.[178] As soon as a device collects data that includes content, the device is not a pen register. If the device is not a pen register, the limitation does not apply. There are no other circumstances in which the limitation would apply, because the limitation only applies to pen registers that collect data that might include content. Thus, this theory essentially writes the limitation out of the statute.

In sum, applying the canons of interpretation fails to cure the ambiguity of the Pen/Trap Statute because each of the three theories appears equally prone to criticism. Although one additional canon is

---

[174] ROBERT E. RODES, JR. & HOWARD POSPESEL, PREMISES AND CONCLUSIONS: SYMBOLIC LOGIC FOR LEGAL ANALYSIS 51 (1997) ("One who gives this argument a superficial examination may hold that it exhibits the form *modus tollens*. Closer inspection, however, will show that it is the counterfeit of *modus tollens*, the invalid pattern called the *fallacy of denying the antecedent*."); *see also* Supp. Amicus Brief, July '07, *supra* note 170, at *33-*34.

[175] RODES & POSPESEL, *supra* note 174, at 51.

[176] *See supra* notes 147-148 and accompanying text.

[177] *See supra* note 168 and accompanying text.

[178] *See supra* note 153 and accompanying text.

discussed below in Part II.D, before proceeding to that discussion, Part II.C briefly examines the legislative history of the statute for additional signs of legislative intent.

C. The Legislative History of the Pen/Trap Statute

When confronted with an ambiguous statute, courts often resort to legislative history in order to ascertain the effect that Congress intended the statute to have.[179] The process of using legislative history has its critics.[180] Nevertheless, courts routinely resort to legislative history, despite academic critiques of its utility. Among proponents of legislative history, committee reports are generally viewed as the most persuasive form of legislative history.[181] Statements made by individual senators are less persuasive than committee reports,[182] however, statements made by a bill's sponsor are typically considered more persuasive than the remarks of other Congressmen.[183]

As noted previously, the legislative history of CALEA concerning the passage of the 1994 amendment that enacted the limitation is ambiguous.[184] Statements in the Senate and House Reports and statements made directly by Senator Leahy[185] alternate between indicating that the limitation envisioned minimal collection of content, and indicating that it did not.[186] No clear answer to the question of whether Congress intended a pen register to collect PCTDDs that contain a minimal amount of content emerges by resorting to legislative history from 1994.

The legislative history related to the passage of the USA PATRIOT Act in 2001 is equally unhelpful. Unlike the 1994 amendments, no committee reports address the intended effect of the amendments of § 216.[187] However, Senator Leahy made remarks bearing directly on the intended effect of § 216 on the Pen/Trap Statute.[188]

---

[179] *See, e.g.*, Kosak v. United States, 465 U.S. 848, 855-57 (1984); *see also In re* Sinclair, 870 F.2d 1340, 1342 (7th Cir. 1989).

[180] *See* SCALIA, *supra* note 82 and accompanying text; *see also* Piper v. Chris-Craft Indus., Inc., 430 U.S. 1, 26 (1977).

[181] ESKRIDGE ET AL., *supra* note 159, at 981; *see, e.g.*, Blanchard v. Bergeron, 489 U.S. 87, 91-96 (1989); United States v. UAW-CIO, 352 U.S. 567, 585-86 (1957).

[182] ESKRIDGE ET AL., *supra* note 159, at 1020.

[183] *Id.* at 1000 (suggesting that the "statements by sponsors are given such deference in part because the sponsors are the most knowledgeable legislators about the proposed bill and in part because their representations about the purposes and effects of the proposal are relied upon by other legislators").

[184] *See supra* notes 117-125 and accompanying text.

[185] Senate Report 103-402 accompanied the Digital Telephony Bill of 1994. S. REP. No. 103-402, at 10 (1994). No senate report was submitted with CALEA. H.R. REP. No. 103-827, at 1 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3489.

[186] *See supra* notes 120-125 and accompanying text.

[187] Government's Memorandum of Law in Support of Its Requests for Authorization to Acquire Post-cut-through Dialed Digits Via Pen Registers at 26-27, *In re* Orders (1) Authorizing Use of Pen Registers and Trap and Trace Services and (2) Authorizing Release of Subscriber

This legislative history can be viewed in two distinct ways. Both ways agree on certain fundamental points. First, it is evident that in 1994, members of Congress recognized that pen registers could collect content,[189] and that in 2001, members of Congress recognized that pen registers routinely did collect content.[190] Second, it is evident that in 2001, members of Congress recognized that the government based its authority to collect PCTDDs that contained content on its interpretation of the 1994 limitation embodied in 18 U.S.C. § 3121(c).[191] Third, it is evident that with these first two factors in mind, Congress enacted legislation that amended three provisions of the Pen/Trap Statute, including the limitation itself, with language that prohibited the use of a pen register to collect content.[192]

With this in mind, it is possible to view the Pen/Trap Statute from an "aerial" perspective. The evolution of the statute over time—from its inception in 1986 to the 1994 and 2001 amendments—is consistent with a desire by Congress to protect the content of electronic communications despite the advent of new technologies that threatened that status.[193] When Congress realized in 1994 that pen registers could collect content, it enacted the limitation. When Congress realized that the limitation did not prevent the collection of content in practice, it enacted three additional provisions intended to prohibit the collection of content.[194] From this history, it is possible to conclude as a general matter that the three amendments point towards a singular conclusion, namely that, "interception of any communications content is not authorized, and technology must be used to insure that communications content is not collected."[195] If viewed in this way, the legislative history supports the denial of an application to install and use a pen register to collect all digits dialed from a subject telephone.[196]

On the other hand, by placing more emphasis on the specific circumstances surrounding the 2001 amendments, arguments to the contrary emerge. It is apparent that in 2001, Senator Leahy believed that the collection of content by a pen register was unconstitutional.[197] However, that Senator Leahy held this belief does not mean that each

---

Information, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (No. 06 Misc. 547, No. 6 Misc. 561), 2007 U.S. Dist. Ct. Br. LEXIS 545, at *26-*27 [hereinafter Gov't Brief, Jan. '07].

188 147 CONG. REC. S10,990, S10,999 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

189 *See e.g.*, Freeh Statement, *supra* note 119, and accompanying text.

190 147 CONG. REC. at S11,000 (statement of Sen. Leahy).

191 *Id.*

192 *See supra* notes 132-135 and accompanying text.

193 *S.D. Tex. I*, 441 F. Supp. 2d 816, 826 (S.D. Tex. 2006).

194 *Id.*

195 *Id.* at 827.

196 *See In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 333-34 (E.D.N.Y. 2007).

197 147 CONG. REC. S10,990, S11,000 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

member of Congress shared it. In fact, Senator Leahy's remarks indicate that during the process of reaching consensus on the provisions of the bill, he encountered and acquiesced to resistance to his efforts to add additional protection for PCTDDs that contain content. Examining the compromises made between parties with distinctly different viewpoints about a divisive issue is an important way of gauging the effect that Congress intended the statute to have.

For instance, Senator Leahy proposed that the PATRIOT Act should include specific definitions for the terms "routing" and "addressing" to ensure that courts did not interpret the terms so broadly that they included content.[198] Yet, the Bush Administration and the Department of Justice "flatly rejected" that approach.[199] Senator Leahy worried that the Administration's desire to leave the terms undefined would fail to protect content.[200] But Congress did not decide to include definitions in the statute. Instead, Congress and the Administration reached a compromise that included amending the definitions of a pen register and trap-and-trace device and the limitation to prohibit the collection of content. Thus, although Senator Leahy personally believed that content collection under the statute should be prohibited, his statements indicate that the statute did not follow a path that would have unequivocally achieved this effect. It follows that because the amendments represented a compromise between Senator Leahy and the Administration, they should not be viewed as adopting only Senator Leahy's view and absolutely prohibiting the collection of content.[201]

Driven by his concerns about content collection, Senator Leahy also sought to update and modify the judicial review procedure for obtaining authorization to install and use a pen register by requiring law enforcement agents to present details of their investigations to the judges who consider their applications. Senator Leahy did not argue that the relevance standard should be enhanced, but only that courts should learn more information about the underlying investigations.[202] Again, Senator Leahy met with defeat. The Bush administration refused to capitulate, and Senator Leahy acquiesced, but nevertheless appeared satisfied with the final result.[203] This progression carries two implications. First, it

---

198 *Id.*

199 *Id.*

200 *Id*.

201 For a discussion that highlights the importance of identifying legislative compromises, see ESKRIDGE ET AL., *supra* note 159, at 67 ("[T]he existence of vetogates may tell statutory interpreters . . . to whom they should pay attention if they consult legislative history . . . . Legislative statements are most important when they reflect assurances by the enacting coalition—especially promises to or by gatekeepers—to enable the bill to pass through a vetogate.").

202 147 CONG. REC. at S11,000 (statement of Sen. Leahy).

203 *Id.*; *see also id.* at S11,015 (statement of Sen. Leahy) ("It is not precisely the bill I would have written . . . . But it is a good bill. It is a balanced bill. . . . It is one that sets up the checks and balances necessary in a democratic society that allow us to protect and preserve our security but also protect and preserve our liberties.").

appears that if the statute required more disclosure, then Senator Leahy would have been comfortable if courts continued to grant pen register applications on the low relevance standard, despite the fact that pen registers were known to collect content. Second, the legislation that finally passed did not reflect only Senator Leahy's vision of how the statute would operate, but also took into account the perspective of the Bush Administration, which viewed the collection of PCTDDs that contain content favorably.

Lastly, Senator Leahy also acknowledged that the FBI had reported that it continued to collect content because there had been no change in technology that would "better restrict" the information collected so as to include only non-content.[204] The FBI's use of the phrase "better restrict" indicates that it sought to develop technology that would screen content more efficiently, but not completely. Yet despite being made aware of the FBI's perspective, neither Senator Leahy nor Congress categorically rejected the possibility that a pen register could collect minimal content if technology could "better restrict" that process. Nor did Senator Leahy express any intention to modify or eliminate the limitation, which was known to be the basis of the government's claimed authority to collect PCTDDs that contain content.[205]

In sum, the legislative history of the Pen/Trap Statute is amenable to two interpretations. On the macro level, the evolution of the Pen/Trap Statute, culminating in the passage of three distinct amendments that prohibited the collection of content, supports the conclusion that Congress intended to prevent the collection of content by a pen register. On the micro level, the legislative history demonstrates that the amendments that emerged from the legislative process resulted from compromises between those who advocated greater protection for content and those who rejected greater protection for content. Thus, Congress did not intend the amendments to protect content completely. Because this history lends equal support to both outcomes, it cannot be dispositive on the question of whether the Pen/Trap Statute authorizes the collection of content with a pen register.[206]

D. Applying the Canon of Constitutional Avoidance to the Pen/Trap Statute

A stronger argument in support of the conclusion that the Pen/Trap Statute does not authorize the collection of content lies in

---

[204] *Id.* at S11,000 (statement of Sen. Leahy).

[205] Gov't Brief, Jan. '07, *supra* note 187, at *31-*32.

[206] *See, e.g.*, Landgraf v. USI Film Prods., 511 U.S. 244, 262-63 (1994) (refusing to view legislative history as dispositive of Congressional intent in the absence of evidence that members of Congress believed that they had reached a tacit agreement to a controversial issue).

applying the canon of constitutional avoidance.[207] This canon has been described as "the preeminent canon of federal statutory construction."[208] It guides courts choosing between competing interpretations of a statutory text to choose an interpretation that avoids raising a constitutional question.[209] To apply the canon, a court need not determine that a particular statutory interpretation would undoubtedly conflict with the Constitution. Rather, a court must only conclude that the interpretation might be unconstitutional, and then avoid it.[210]

Congress has historically gone to great lengths to ensure that the Fourth Amendment protects the content of electronic communications.[211] Further, the Supreme Court has given no indication that the content of electronic communications is entitled to less protection when it is conveyed over a telephone in the form of PCTDDs than when it is conveyed through other means that require compliance with Title III's procedures. Nevertheless, the government has argued that a telephone user cannot maintain a reasonable expectation of privacy after entering such digits into an automated telephone system.[212] The government reaches this result by extending the holding in *Smith*. Under its view, a caller assumes the same risk with respect to PCTDDs as with respect to the digits dialed to connect a telephone call because both types of digits must be conveyed to the telephone company, which can in turn record all of the digits dialed.[213] It follows from this interpretation that no dialed digits are entitled to Fourth Amendment protection.[214]

Yet at its outset, *Smith* acknowledged that its holding did not address the government's ability to capture the content of communications.[215] Rather, *Smith* presupposed a context in which a pen register intercepted non-content digits voluntarily transmitted to a telephone company in order to complete a call, but could not intercept content.[216] The PCTDD issue today has arisen squarely outside *Smith's* framework. It exists within a fundamentally different context and

---

[207] *In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 335 (E.D.N.Y. 2007).

[208] Adrian Vermeule, *Saving Constructions*, 85 GEO. L. J. 1945, 1948 (1997).

[209] *See, e.g.*, Clark v. Martinez, 543 U.S. 371, 380-82 (2005); *see also* Harris v. United States, 536 U.S. 545, 555 (2002).

[210] Vermeule, *supra* note 208, at 1958.

[211] *E.D.N.Y. I*, 515 F. Supp. 2d at 335-36; *see also* Kerr, *supra* note 69, at 630-31.

[212] Brief for Gov't, *In re* Orders (1) Authorizing Use of Pen Registers, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (No. 06-Misc.-547, 561, 07-Misc.-120), 2007 U.S. Dist. Ct. Br. LEXIS 539, at *2.

[213] *Id*.

[214] *Id*.

[215] Smith v. Maryland, 442 U.S. 735, 741 (1979) ("[P]en registers do not acquire the *contents* of communications.").

[216] *Id.* at 741-42.

presents constitutional concerns that *Smith* did not foresee.[217] Consequently, it is doubtful whether *Smith's* holding governs the interception of content with a pen register at all. It is even more doubtful whether extending *Smith* in order to justify the collection of content under the Pen/Trap Statute would be constitutional, for the simple fact that Congress has repeatedly recognized that the Fourth Amendment protects the content of electronic communications.[218] For these reasons, the government's interpretation should be avoided under the canon of constitutional avoidance.

Even a court that applied *Smith* to PCTDDs would reach the same result. *Smith* applied the test articulated in *Katz*, which determines whether a particular form of electronic surveillance violates the Fourth Amendment.[219] Under *Katz*, the person invoking Fourth Amendment protection must demonstrate a justifiable, reasonable, or legitimate expectation of privacy in the information sought to be protected.[220] This inquiry is normally satisfied by demonstrating both that an individual exhibited an actual expectation of privacy, and also that the individual's subjective expectation is one that society is prepared to recognize as reasonable.[221]

In light of *Katz*, the government's argument is unavailing because it fails to consider the actual nature of PCTDDs. Both *Katz* and Congress have emphasized that the content of a communication is entitled to Fourth Amendment protection.[222] Despite the expectations of privacy that people maintain in their bank account numbers, social security numbers, or other private information,[223] the government's theory associates PCTDDs most closely with digits dialed to connect a call. Yet, when they contain substantive, private information, PCTDDs actually resemble the content that *Katz* sought to protect.[224] When a telephone user enters PCTDDs to navigate an automated answering system, the PCTDDs are the equivalent of a conversation with an entity

---

[217] *See, e.g.*, 147 CONG. REC. S10,990, S11,000 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

[218] 18 U.S.C. § 2510(8) (2006); *see also* Supp. Amicus Brief, July '07, *supra* note 170, at *27-*28.

[219] *See supra* note 45 and accompanying text.

[220] Smith v. Maryland, 442 U.S. 735, 739 (1979).

[221] *Id*. *But see id.* at 740 n.5 (noting that "where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was").

[222] *See supra* notes 38, 50-51 and accompanying text.

[223] *In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 336 (E.D.N.Y. 2007).

[224] *Id*.

representative that would otherwise be protected.[225] Without a wiretap order, a pen register cannot lawfully intercept the oral component of telephone conversations. Similarly, a pen register should not be able to intercept lawfully the functional equivalent of an actual conversation simply because it takes the form of a PCTDD.[226] To conclude otherwise would interfere with telephone users' legitimate expectation of privacy in PCTDDs that contain content.

Finally, in *Smith*, the Court rejected the petitioner's privacy claim because it imputed to telephone users, as a class, notice that dialed digits may be monitored, which bolstered its conclusion that one who dials a telephone assumes a known risk that those digits might be provided to the government.[227] Yet while the third-party disclosure principle supplies grounds for eliminating Fourth Amendment protection,[228] its application in *Smith* rests on the assumption that a reasonable user will know that he is revealing information in a manner that can lead to its interception.[229] It is a stretch to say that the telephone user assumes the risk that digits dialed into an automated system after being connected to the target number will be monitored by the telephone company,[230] because the telephone user receives inadequate notice that such a risk exists.[231] For instance, PCTDDs are not listed on monthly bills like digits dialed to connect a call.[232] Nor would a telephone user have

---

[225] Michael A. Rosow, Note, *Is "Big Brother" Listening? A Critical Analysis of New Rules Permitting Law Enforcement Agencies to Use Dialed Digit Extraction*, 84 MINN. L. REV. 1051, 1073 (2000).

[226] *Id.* at 1078. PCTDDs can also be analogized to the digits transmitted to pagers. *E.D.N.Y. I*, 515 F. Supp. 2d at 339. Courts considering the question have held that the Fourth Amendment protects digits transmitted to pagers. *See, e.g.*, Brown v. Waddell, 50 F.3d 285, 294 (4th Cir. 1995).

[227] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[228] *See supra* note 69-70 and accompanying text.

[229] *Smith*, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").

[230] It is beyond the scope of this Note to evaluate a debate between the Federal Defenders of New York and the Government about whether the particular way in which PCTDDs are transmitted should factor into the determination of whether the Fourth Amendment protects them. *Compare* Supp. Amicus Brief, July '07, *supra* note 170, at *5-*6 (distinguishing between the transmission of digits over the control channel and content channels), *with* Gov't Brief, June '07, *supra* note 141, at *9-*10 (minimizing the distinction between the control and content channels). For technical information about digital telephony technology, see *Communications Assistance for Law Enforcement Act: Hearing Before the FCC* (1999) (statement of Dave Yarbaugh, FBI Supervisory Special Agent), *available at* http://www.askcalea.net/lef/docs/990127-y.pdf; *see also Communications Assistance for Law Enforcement Act: Hearing Before the FCC* (1999) (statement of John W. Cutright, FBI Electrical Engineer), *available at* http://www.askcalea.com/lef/docs/990127-c.pdf..

[231] Further, such a risk is not consonant with the expectations of privacy that the telephone user would retain if the same information was transmitted by conversation. On the other hand, that the Fourth Amendment would not protect digits dialed to connect a telephone call is consonant with the fact that automated dialing systems are the functional equivalent of live operators, to whom the user willingly revealed the destination telephone number. *Smith*, 442 U.S. at 744-45.

[232] Rosow, *supra* note 225, at 1078.

any reason to expect a continued need for monitoring by the telephone company beyond the point of connection to a third party's line.[233]

In *Smith*, the Court identified multiple ways in which the telephone user received notification of the telephone company's capacity to monitor digits dialed to connect calls.[234] Because it was reasonable to conclude that the telephone user received notice that such practices could occur, the Court concluded it was unreasonable to believe that a telephone user expected communications to be private.[235] Yet the Court did not and has never held that a telephone user assumes the risk that communications may be revealed solely because the telephone company possesses the capacity or occasionally chooses to monitor electronic transmissions. Notice to the user—at least sufficient to impute knowledge—is also a necessary element of the assumption of risk argument. To conclude otherwise would achieve the result that *Smith* rejected by conditioning Fourth Amendment protection on the particular industry practices of the service provider, without regard for a reasonable user's actual or imputed knowledge of those practices.[236] By this logic, even the content of actual conversations could be revealed by a pen register, since the telephone company has the capacity to monitor conversations.[237]

In sum, telephone users have a reasonable expectation of privacy in PCTDDs that contain content. Society generally and Congress in particular have traditionally regarded the content of electronic communications as private. Further, telephone users do not voluntarily assume the risk that content transmitted via telephone in the form of a PCTDD will be revealed to the government. In light of this, the Fourth Amendment protects PCTDDs that contain content. Therefore, under the canon of avoidance, the Pen/Trap Statute should not be interpreted to permit the collection of content, since such an interpretation would bring the statute into conflict with the United States Constitution.

III. AMENDING THE PEN/TRAP STATUTE

Interpreting the Pen/Trap Statute to permit the collection of content will create constitutional problems and may violate the Fourth

---

[233] *Smith*, 442 U.S. at 742-43 (identifying commonly known reasons that a telephone company monitors dialed digits, including "to aid in the identification of persons making annoying or obscene calls").

[234] *See supra* note 71 and accompanying text.

[235] *Smith*, 442 U.S. at 742-43.

[236] *Id.* at 745.

[237] *Id.* at 746 (Stewart, J., dissenting) (A "telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment."). Title III provides an exception for such practices. 18 U.S.C. § 2511(2)(a)(i) (2006); *see also In re* United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Info. (*E.D.N.Y. I*), 515 F. Supp. 2d 325, 338 (E.D.N.Y. 2007).

Amendment.[238] Although a preferable approach is to interpret the Pen/Trap Statute to prohibit the collection of content, to some extent this may limit the utility to law enforcement agencies of a valuable investigative tool.[239] Both options have drawbacks. Therefore, the Pen/Trap Statute requires immediate attention from Congress.

This Part identifies possible methods for amending the Pen/Trap Statute that balance the need to adequately protect privacy expectations with law enforcement's ability to use pen registers in the course of conducting investigations. In Part A, this Note suggests several courses of action intended to redress the statutory ambiguity created by the 1994 limitation. In Part B, this Note reiterates suggestions made by other commentators that apply to the Pen/Trap Statute more generally.

A. Amending the 1994 Limitation in 18 U.S.C. § 3121(c)

1. Articulate the Consequences of a Lack of Reasonably Available Technology

The interpretive tension in the Pen/Trap Statute results from the interplay between the statutory definition of a pen register in 18 U.S.C. § 3127(3) and the 1994 limitation reflected in 18 U.S.C. § 3121(c).[240] The definition provides that pen registers shall not collect content. The limitation contains a positive commandment to use reasonably available technology to sort content from non-content, but fails to articulate the consequence of an absence of such technology. This failure allows the statute to be interpreted to permit the collection of content.

If the limitation remains in the statute, then amending the limitation to include language that articulated the effect of an absence of reasonably available technology to sort content from non-content would effectively resolve the ambiguity of the statute. It would also end the divisive speculation into the effect of the limitation and the fruitless debate about Congress's intention in passing the various amendments to the Pen/Trap Statute over the past several decades.

Congress must articulate the effect of an absence of reasonably available sorting technology. To align the limitation with the considerations discussed in this Note, any additional statutory language should continue to reflect the policies of the PATRIOT Act and prohibit the collection of content. One option would be to provide that in the absence of reasonably available technology, the pen register shall be restricted to collecting the first ten digits of any numbers dialed. This

---

[238] *See supra* Part II.D.

[239] *See E.D.N.Y. I*, 515 F. Supp. 2d at 339; *see also S.D. Tex. I*, 441 F. Supp. 2d 816, 825 (S.D. Tex. 2006).

[240] *See generally* Part II.B.

would effectively prevent pen registers from collecting PCTDDs.[241] The government currently possesses technology that enables it to record a specified number of dialed digits.[242] Should the government utilize that technology to record ten digits, it could use those ten digits to identify calls that a telephone user placed to calling card companies. The government could in turn subpoena the calling card provider directly in order to determine the final destination to which the call was routed, rather than the telephone service provider, in order to collect non-content PCTDDs,[243] to which it would be entitled under the Pen/Trap Statute.

This solution would impose a greater administrative burden on the government. However, this burden would provide a positive incentive to develop technology to sort PCTDDs. The current statutory regime disincentives such research and development because the government faces no adverse consequences as a result of continuing to collect PCTDDs that contain content. In fact, the government may even have a perverse incentive to avoid developing technology to sort PCTDDs containing content from those that do not, in order to continue obtaining all PCTDDs for as long as possible.[244]

2. Modify or Eliminate the Reasonably Available Technology Provision

A second alternative is to modify the limitation by deleting the technology reasonably available exception. One significant benefit of this option is that it would minimize the risk of future constitutional violations by creating an unequivocal prohibition on the collection of content. For instance, the government's interpretation of the Pen/Trap Statute would be diffused if Congress struck language from the current version of 18 U.S.C. § 3121(c) in the following manner:

> (c) Limitation.—A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology ~~reasonably available~~ to ~~it that~~ restrict~~s~~ the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.[245]

---

[241] To date, one law enforcement agency adopted this strategy, agreeing to configure its computers to automatically delete all PCTDDs received from the telephone service provider. This mooted the legal question of whether the pen register could collect all PCTDDs. United States for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices (*E.D.N.Y. II*), No. 08-308, 2008 U.S. Dist. LEXIS 97359, at *3-*4 (E.D.N.Y. Nov. 22, 2008).

[242] *S.D. Tex. I*, 441 F. Supp. 2d at 825.

[243] Supp. Amicus Brief, July '07, *supra* note 170, at *13.

[244] 147 CONG. REC. 10,990, S11,000 (daily ed. Oct. 25, 1001) (statement of Sen. Leahy); *see also* Supp. Amicus Brief, July '07, *supra* note 170, at *36 n.13.

[245] 18 U.S.C. § 3121(c) (2006) (alterations to original). The alterations appearing in the block quote are intended to serve an illustrative purpose.

The drawback to this suggestion is that the limitation would be superfluous. Since the definition of a pen register excludes any device that is capable of collecting content, it goes without saying that the government should use technology that prevents it from collecting content when acting under the authority of the Pen/Trap Statute. If the limitation merely reiterated this conclusion, it may as well not be included in the statute.

Therefore, another possibility that would confer the same benefit is to eliminate the limitation in 18 U.S.C. § 3127(c) altogether. The limitation is unnecessary if the definition of a pen register contains a plain prohibition on the collection of content. Further, if no reasonably available technology can sort content from non-content, then the limitation does nothing but muddle the statutory text. The limitation only applies to a set of circumstances that do not exist. Meanwhile, the limitation creates ambiguity by failing to address the circumstances at hand. It appears that the primary function of the limitation is to create confusion.

With the limitation removed from the statutory text, the statutory definition of a pen register would plainly prohibit the collection of content. While this result would temporarily decrease the utility of a pen register for law enforcement agencies, it would not prevent them from obtaining content-based PCTDDs pursuant to other valid methods. For instance, with a showing of probable cause, the government would still be able to obtain a wiretap warrant to intercept PCTDDs.[246] In addition, the method of restricting the collection of digits dialed to ten would also be available. Further, as soon as the government developed technology to sort content from non-content, it would employ that technology to avoid collecting content, even without the limitation. In other words, the limitation is not an essential component of the Pen/Trap Statute and could be eliminated with no significant negative repercussions.

B. Broad Amendments to the Pen/Trap Statute

1. Allow Judicial Review

Currently, 18 U.S.C. § 3123(a) provides that the court "shall" authorize a pen register upon certification by a government representative of its relevancy to an investigation.[247] For so long as pen registers can collect content, Congress should amend this section in order to allow for judicial review during the consideration of a pen register

---

[246] *S.D. Tex. I*, 441 F. Supp. 2d at 818; *see also* United States for an Order Authorizing the Installation and Use of an Elec. Computerized Data Collection Device Equivalent to a Pen Register and Trap and Trace Device, No. 06:06-mj-1130 at 6 (M.D. Fla. June 20, 2006) ("[T]he government is not without a remedy: if it decides that obtaining post-cut-through digits is sufficiently important to its criminal investigation, it may submit a wiretap application.").

[247] 18 U.S.C. §§ 3122(b), 3123(a) (2006).

application. Senator Leahy has advocated that the standard for judicial review should be heightened to provide courts a degree of independent latitude.[248] Instead of relying on a law enforcement agent's certification that the digits sought to be collected are relevant to an investigation, the court could review the facts for itself to determine whether that was indeed the case. This solution will not minimize the likelihood that the use of a pen register will create a constitutional conflict, since pen registers will still be capable of collecting content. However, granting courts the power of judicial review will at least add oversight to the application process and may prevent the collection of content where the justification for such collection is weak.

2. Heighten the Standard of Proof

Alternatively, the House Judiciary Committee has proposed that Congress modify the Pen/Trap Statute to provide that before a pen register can be ordered and installed, the government must demonstrate "specific and articulable facts [that] reasonably indicate that a crime has been, is being, or will be committed, and [that] information likely to be obtained by such installation and use . . . is relevant to an investigation of that crime."[249] Another option suggested by one commentator is to raise the relevancy standard so that pen registers can only be authorized pursuant to a greater showing of suspicion, such as the "clear and convincing evidence" standard that applies to requests for disclosure of cable records under the Cable Communications Policy Act.[250] It is clear that either of these options, if adopted, would improve the status quo.

3. Provide a Suppression Remedy

If Congress does not eliminate the limitation, it should amend the Pen/Trap Statute with a provision that provides for the suppression of any PCTDDs collected or decoded by a pen register that represent content.[251] Currently, the government is under no mandate to discard content collected with a pen register and courts routinely admit evidence collected by pen registers, even if that evidence was collected in an unlawful manner.[252] Although the government's official position is not to

---

[248] 147 CONG. REC. at S11,000 (statement of Sen. Leahy).

[249] *Id.* (citing Report 106-932, 106th Cong. 2d Sess. 13, Oct. 4, 2000). The Bush Administration rejected adding this proposed language to the statute. *Id.* Another commentator has suggested amending the standard of proof in the context of Internet surveillance using a pen register. *See* Ditzion, *supra* note 12, at 1351 ("[A] higher standard for approving Internet pen register orders should be established.").

[250] Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1437 (2004).

[251] *See* Ditzion, *supra* note 12, at 1348-49 (suggesting ways to clarify and improve pen register laws); *see also* Bankston, *supra* note 138, at 631.

[252] *See supra* note 105 and accompanying text.

make affirmative use of content, agents of the DOJ have also received instructions to store records of all content collected indefinitely.[253] By amending the Pen/Trap Statute to mandate the suppression of content collected with a pen register, Congress would ensure that content collected under a mere relevance standard cannot be used against a telephone user. This would minimize the risk of harm flowing from the constitutional violation of collecting content with a pen register. It would also harmonize the Pen/Trap Statute with Title III, which provides for the suppression of the content of oral or wire communications intercepted unlawfully.[254]

4. Increased Transparency About the Installation and Use of Pen Registers

Any discussion of pen registers is limited by a lack of information.[255] There is no meaningful account of the number of applications to install and use a pen register made each year. Likewise, there is no accessible record of the number of applications to install and use a pen register granted or denied by courts.[256] Although anecdotal evidence indicates that law enforcement agencies install and operate thousands of pen registers each year,[257] it is impossible to fully appreciate the significance of the government's ability to collect content under the Pen/Trap Statute without knowing how often this practice occurs. To cure this lack of transparency, the Pen/Trap Statute should be updated to require an annual report about the government's use of pen registers.[258]

As with the proposed suppression remedy, Title III provides a fitting model for updating the reporting requirements of the Pen/Trap Statute.[259] Congress should require the appropriate officials to report annually to the Administrative Office of the United States Courts comprehensive details about pen register applications,[260] including the percentage of pen register orders that authorize the collection of all digits dialed from a particular telephone number, as distinguished from those orders that restrict the collection of PCTDDs to dialing information.[261]

---

[253] Thompson Memo, *supra* note 141 and accompanying text.

[254] 18 U.S.C. § 2515 (2006).

[255] Bankston, *supra* note 138, at 634 (emphasizing that "only the DOJ" knows the extent of electronic surveillance carried out under the authority of the Pen/Trap Statute).

[256] *Id*. On the other hand, information about the total number of wiretap applications approved each year is readily accessible. *See* http://www.uscourts.gov/library/wiretap.html (last visited Feb. 5, 2009).

[257] *See supra* notes 13-14.

[258] Bankston, *supra* note 138, at 633 (suggesting the same solution).

[259] 18 U.S.C. § 2519 (2006).

[260] *Id.* § 2519(2) (2006).

[261] Records reflecting this distinction would show whether a judicial consensus to restrict the collection of PCTDDs was emerging over time. *See, e.g.*, United States for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices (*E.D.N.Y. II*), No. 08-308, 2008 U.S. Dist. LEXIS 97359, at *3-*4 (E.D.N.Y. Nov. 22, 2008).

Further, that office should forward a final report to Congress to allow for further consideration of the pen register issue.[262] Knowing that detailed information was being compiled would presumably increase judicial awareness of the questionable uses to which pen registers can be put. In turn, this awareness might encourage meaningful discourse on the subject, as well as prompt Congressional action to more effectively balance the need for vigorous law enforcement with the Fourth Amendment's protections.

IV. CONCLUSION

Telephone users have a reasonable expectation of privacy in the content of their electronic communications. This expectation includes content that takes the form of a PCTDD. The expectation is also one that society is prepared to recognize as reasonable. As with other forms of communicative content, interception of PCTDDs that contain content is not lawful on a showing of less than probable cause. For these reasons, the collection of content on the mere relevance standard provided by the Pen/Trap Statute should be prohibited.

Nevertheless, until Congress takes steps to do so, the government will continue to solicit and receive court authorization to install and use pen registers in a manner that will result in the collection of content. The time is ripe for Congress to amend the Pen/Trap Statute in order to cure its ambiguities and impose an effective barrier to the continued practice of collecting PCTDDs that contain content using a pen register.

Marcus M. Baldwin[†]

---

[262] *Id.* § 2519(3) (2006).

[†] J.D. Candidate, 2009; A.B. Cornell University, Jan. 2002. Many thanks to Paul Monteleoni and Daniel Bodah, to Professor Brakman Reiser, and to the staff members of the *Brooklyn Law Review*.